uniFLOW Online Customer Contract

ATTACHMENT 1 – DATA PROCESSING AGREEMENT

Contents

Data Processing Agreement

(Software as a Service)

This data processing agreement (the **"Data Processing Agreement"**) forms part of the (the **"Agreement"**) and is entered into between NT-ware Systemprogammierungs GmbH, a limited liability company registered in Germany having its principal place of business at Niedersachsenstraße 6, Bad Iburg, Germany, 49186 (**"NT-ware"**) and the customer identified on the signature page of the Agreement (**"Customer"** – together the **"Parties"**).

1. DEFINITIONS

Unless otherwise defined herein, all capitalised terms shall have the same meaning as in the Agreement.

"**Data Protection Legislation**" means the General Data Protection Regulation and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including the General Data Protection Regulation), and all other applicable laws relating to processing of personal data and privacy that may exist in any relevant jurisdiction, including, where applicable, the guidance and codes of practice issued by supervisory authorities;

"**General Data Protection Regulation" or "GDPR**" means the General Data Protection Regulation (EU) 2016/679; and

"**Security Breach**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

"**Services**" means the uniFLOW Online Cloud Services Services as further defined in the Agreement.

"**Standard Contractual Clauses**" means the Standard Contractual Clauses for Data Processors established in third countries pursuant to European Commission Decision (2010/87/EU) of the Data Protection Directive, as currently available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087 (or any subsequent version thereof released by the European Commission; the latest version shall automatically apply). Schedules 1 and 2 to this Data Processing Agreement form part of the Standard Contractual Clauses as Appendices 1 and 2.

"**data controller**", "**data processor**", "**data subject**", "**personal data**", "**processing**" and shall be interpreted in accordance with the General Data Protection Regulation.

2. GENERAL

2.1. This Data Processing Agreement shall apply to the extent NT-ware is processing in the course of providing the Services personal data on behalf of the Customer within the meaning of Art. 4 No. 2 and Art. 28 GDPR.

2.2. This Data Processing Addendum serves as a data processing agreement between NT-ware and each data controller providing personal data under the Agreements with view to the personal data that NT-ware processes in the course of providing the Services.

2.3. The Parties agree that the Customer and the Customer Affiliates covered by the Agreement are the data controllers and NT-ware is the data processor in relation to the personal data that NT-ware processes in the course of providing the Services.

3. PERSONAL DATA PROCESSING

3.1. The subject-matter of the data processing is the performance of the Services and the processing will be carried out for the duration of the Agreement. The obligations and rights of the Customer and Customer Affiliates are as set out in this Data Processing Agreement. Schedule 1 of this Data Processing Agreement sets out the nature and purpose of the processing, the types of personal data the NT-ware processes and the categories of data subjects whose personal data is processed.

3.2. Customer shall be solely responsible for compliance with applicable Data Protection Laws with view to the processing that takes place under this Data Processing Agreement, in particular that Personal Data is disclosed to NT-ware and that personal data is processed by NT-ware on behalf of Customer.

3.3. To the extent Affiliates of the Customer are also covered by the Services under the Agreement and Customer acts in this respect on behalf of and in the name of its Affiliates (Data Controllers),

   3.3.1. Customer will serve as a single point of contact for NT-ware (NT-ware may refuse any instructions provided directly by a Data Controller that is not the Customer);

   3.3.2. Customer is solely responsible for the coordination, submission and assessment of any instructions of Data Controllers that are not the Customer to NT-ware;

   3.3.3. Customer shall enter into data processing agreements with all other Data Controllers covered by this Data Processing Addendum in order to enable NT-ware and its Subprocessors to process personal data as described in this Data Processing Agreement; and

   3.3.4. Customer warrants to NT-ware that its instructions, including appointment of NT-ware as a Data Processor or Sub-processor, have been authorized by the relevant Affiliate/Data Controller.

3.4. When the NT-ware processes personal data in the course of providing the Services, NT-ware shall, notwithstanding anything to the contrary in this Agreement:

   3.4.1. process the personal data only in accordance with written instructions from the Customer on its own behalf or on behalf of its Affiliate in case they are covered by the Agreement as set out exclusively in the Agreement and this Data Processing Agreement and NT-ware will not use or disclose the personal data for its own purposes except where expressly permitted by Article 28 (3)(a) GDPR. If NT-ware is required to process the personal data for any other purpose by European Union or Member State law to which NT-ware is subject, NT-ware shall inform the Customer and the relevant Customer Affiliate via the Customer of this requirement before the processing, unless that law prohibits this on important grounds of public interest. Any additional or alternate instructions must be agreed to according to the process for amending the Agreement.

3.4.2. be responsible for complying with all Data Protection Laws applicable to its provision of the Services in its role as Data Processor (for the avoidance of doubt, NT-ware shall not be responsible for compliance with any laws applicable to the Customer or the Customer's industry that are not generally applicable to information data processors).

3.4.3. notify the Customer and the relevant Affiliate via the Customer immediately if, in the NT-ware's opinion, an instruction for the processing of personal data given by the Customer or the relevant Affiliate infringes applicable Data Protection Legislation (without any obligation to perform a legal assessment when providing the Services). In that case NT-ware is entitled to suspend the performance of the respective instruction until Customer confirms it lawfulness or modifies such instruction;

3.4.4. implement and maintain appropriate technical and organisational measures to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction, damage or theft of the personal data and having regard to the nature of the personal data which is to be protected. The measures to be taken under this Data Protection Agreement are set out in Annex 2 to this Data Processing Agreement. Customer understands and agrees that these measures are subject to technical progress and development and NT-ware shall be able to implement adequate alternative measures as long as the general security level described in Annex 2 of this Data Processing Addendum is maintained (and not lowered);

3.4.5. at least once per year audit the security of the computers and system environment that it uses for the processing of personal data when providing the Services. Upon Customers written request, NT-ware will provide to Customer a summary of the results of its regular audit ("**Summary Audit Report**"). This Summary Audit report constitutes Confidential Information under the Agreement. Customer agrees to exercise its audit right by instructing NT-ware to execute the audit as described before. If Customer reasonably concludes that an audit at the premises of NT-ware is required, such audits and inspections can be conducted by Customer (or an independent auditor that is no competitor of NT-ware on behalf of the Customer) during

- regular business hours, and without interfering with NT-ware's operations, upon prior;
- notice, and observing an appropriate notice period;
- upon prior notice (observing an appropriate notice period and further consultation with NT-ware),

Such onsite audit is subject to the execution of a confidentiality agreement, in particular to protect the confidentiality of the technical and organisational measures and safeguards implemented by NT-ware. The costs (including internal resources) for the onsite audit should be borne by Customer on an hourly rate based on time and material according to the then current price list.

3.4.6. ensure that access to the personal data is limited to personnel that requires such access to provide Services under the Agreement and personnel required to access the personal data have committed to keep personal data confidential and comply with the obligations set out in this clause and that these confidentiality obligations survive the termination of their engagements) or are under an appropriate statutory obligation of confidentiality;

3.4.7. support Customer in a manner consistent with the functionality of the Services and NT-ware's role as a data processor and to the extent reasonably possible for NT-ware (and only where Customer cannot do so without NT-ware's assistance)

3.4.7.1. in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR; and

3.4.7.2. assist the Customer and the Customer Affiliate via the Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the General Data Protection Regulation (taking into account the nature of the processing and the information available to the NT-ware and provided that this support does not result in any breach of NT-ware's' confidentiality obligations towards third parties).

3.4.8. notify Customer, without undue delay, if NT-ware becomes aware a Security Breach within its scope of responsibility. NT-ware shall implement the measures necessary for securing personal data and for mitigating potential negative consequences for the data subject; NT-ware shall coordinate such efforts with Customer without undue delay;

3.4.9. notify to Customer the point of contact for any issues related to data protection arising out of or in connection with the Agreement;

3.4.10. at the end of the Services upon the Customer's request, securely destroy or return personal data to the Customer and delete existing copies (unless European Union or Member State law requires storage of the personal data);

3.5. Customer shall (i) without undue delay notify NT-ware of any defect or irregularity in terms of data protection compliance when providing the Services and (ii) notify to NT-ware the point of contact for any issues related to data protection arising out of or in connection with the Agreement, and (iii) reasonably support NT-ware in defending possible claims asserted by data subjects against NT-ware or its Affiliates in accordance with Article 82 GDPR.

4. SUB-PROCESSING

4.1. Customer (also on behalf of its Affiliates that are covered by this Data Processing Agreement) authorizes NT-ware to engage Affiliates and third parties to provide the Services and to process personal data as sub-(sub-) processors. This authorisation constitutes the Customer's (and its Affiliates) prior written consent to the sub-processing as required under the Standard Contractual Clauses or the applicable Data Protection Laws. A list of the current subprocessors used to provide the Service is attached to this a Data Processing Agreement as Schedule 3. All these subprocessors will be permitted to process personal data of the Customer (or its Affiliates) only to deliver the Services under the Agreement (unless otherwise stipulated under this Data Processing Agreement). NT-ware remains responsible the subprocessor's compliance with the obligations under this Data Processing Agreement and the applicable Data Protection Laws.

4.2. Subprocessors that are engaged by NT-ware for the provision of the Services shall be subject to written terms with NT-ware that are no less protective than this Data Processing Agreement. Before engaging a third party as subprocessor, NT-ware must evaluate the reliability and competence of this party subprocessor with view to the respective data processing operations that should be performed by the subprocessor (if available based on respective certifications).

4.3. NT-ware shall, prior to the use or replacement of subcontractors with at least 30 days prior notice, inform Customer thereof. Customer shall be entitled to reasonably contradict any change notified by NT-ware within 30 days upon receipt of the Customer's notice and for materially important reasons. The parties will then discuss possible resolutions within 30 days (but without any obligation for NT-ware to implement resolutions suggested by Customer) ("**Resolution Period**"). Where a materially important reason for such contradiction still exists, and the parties are failing to conclude on an amicable resolution of this matter, Company shall be entitled to terminating the Agreement upon 14 days written notice after the Resolution Period has ended. Where Customer fails to contradict such change within such period of time, Customer shall be deemed to have consented to such change. The Customer shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated services. No other claims of the Customer against NT-ware may be based on reason of such termination.

4.4. For the avoidance of doubt, where a third party fails to fulfil its obligations under any sub-processing agreement or any applicable Data Protection Legislation, NT-ware will remain fully liable to the Customer for the fulfilment of the NT-ware's obligations under this Agreement;

4.5. For the avoidance of doubt, the approval requirements under this Data Processing Agreement shall not apply in cases where NT-ware or subprocessors subcontracts ancillary services from third parties which are not specific to the provision of the services under the Agreement. Such ancillary services shall, for example, include (but not be limited to) general infrastructure services like telecommunications services or facility management services. NT-ware and subprocessors shall nevertheless conclude, with such third parties, agreements necessary to ensure applicable data protection standards.

5. THIRD COUNTRY TRANSFER

5.1. In case the processing will be undertaken in a third country (i.e. outside the European Economic Area – "**EEA**"), this will be notified to Customer (for the current list of subprocessors please see Schedule 3). Each and every transfer of data to a country which is not a Member State of either the European Union or the EEA ("**Third Country**") shall only occur if the specific conditions of Article 44 et seq. GDPR have been fulfilled.

5.2. NT-ware has entered into Standard Contractual Clauses with its subprocessor that are situated in a third country unless (i) an adequate level of data protection exists according to an adequacy decision of the European Commission in this country or (ii) a Privacy Shield certification applies to the respective transfer ("**Third Country Transfer**"). In case of a Third Country Transfer, Customer accedes to these Standard Contractual Clauses and agrees that the Standard Contractual Clauses will be enforced against the relevant subprocessor only by NT-ware on behalf of the Customer (and its Affiliates) and commissions NT-ware to do so. Customer will procure that each Affiliate that should be covered by this Data Processing Agreement will likewise accede to these Standard Contractual Clauses and ensure that the enforcement takes place only via NT-ware.

6. LIABILITY AND DAMAGES

The regulations on the parties' liability contained in the Agreement shall be valid also for the purposes of processing under this Data Processing Agreement, unless expressly agreed upon otherwise.

7. MISCELLANEOUS

7.1. This Data Processing Agreement shall automatically terminate upon any termination or expiration of the Agreement.

7.2. In case of any conflict between any provision of this Data Processing Agreement and any provision of the Agreement, this Data Processing Agreement shall prevail. If Standard Contractual Clauses are used according to this Data Processing Agreement and there is a conflict between this Data Processing Agreement and the Standard Contractual Clauses the Standard Contractual Clauses shall prevail.

Schedule 1

Data processing information

The personal data transferred concern the following categories of data subjects:

1. **Data Subjects**

The personal data transferred relate to the following data subjects:

Users and Tenant Administrators of the uniFLOW Online Cloud Services (e.g. employees, agents, applicants and temporary employees of Customer).

2. **Categories of data**

Data will be provided by the Customer (and its affiliates). The personal data transferred may therefore concern different categories of personal data and sensitive data depending on the Customer's use of the Service. This may be e-mail addresses, login data, user names and other which may be required to provide the uniFLOW Online cloud service.

3. **Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data):

See above (prints may contain any data).

4. **Processing operations**

The personal data transferred will be subject to the following basic processing activities:

The personal data transferred will be processed by NT-ware and its sub-processors in order to provide the Services as agreed in the Agreement, such as login functionality, print accounting and report generation. The basic processing activities involve hosting services, maintenance & support services and professional Services.

Schedule 2

Technical and Organisational Measures

Secure Communication

There are various components used in the uniFLOW Online system which communicate amongst each other to provide the service. Communication between the uniFLOW SmartClient and the Canon MEAP device is encrypted via AES-256 RSA. All communication between the uniFLOW Online service and the components on the local network are encrypted via HTTPS.

User Authentication and Password Storage

uniFLOW Online does not store any user credentials such as passwords. Instead, it uses a claims-based approach to authenticate users, accepting logon credentials from multiple identity providers or scan destinations.

The default provider is Microsoft Azure Active Directory. Alternatively, administrators can use Active Directory Federation Services (ADFS) to integrate with e.g. Microsoft Office 365 or their own locally hosted Active Directory®. In addition, it is possible to make use of shared web identity providers like Facebook, Google, Yahoo!® or Windows Live ID.

In order to provide secure scan functionality to each user uniFLOW Online utilizes the same claims-based approach for linking users and their accounts to a scan destination without storing their user credentials.

Tenant Isolation

Each created uniFLOW Online instance is logically separated from other instances via the so-called tenant isolation. That way it can be assured that no personal data is mixed up with data from e.g. other accounts.

Private data is stored in uniFLOW Online according to statutory requirements. By default, private data is not shared with any third parties including Canon or the partner selling the service to the customer. Canon/ the Canon partner can only see names of their customers and expiry dates of licenses. Private data, e.g user names, are only available to the customer.

Whenever data sharing between tenants is wanted, e.g. for analysis, support or service cases, this needs to be enabled by the customer, never via an outside identity. By default, uniFLOW Online will never share any private information.

Data Center

uniFLOW Online is hosted in Microsoft Azure data centers that are distributed across the globe. The use of Microsoft Azure data centers by uniFLOW Online makes it possible to respect data sovereignty as customer data remain within the local region, i.e. European customers' data will always be stored within the European data center in Amsterdam while US customers can be sure their data will never leave the US.

More information about Microsoft Azure and its security and compliance features can be found at the website: https://azure.microsoft.com/en-gb/support/trust-center/

Printing

Print jobs are processed and stored on users' local PCs instead of being sent via the internet to a cloud-based service. With uniFLOW Online printing, all print traffic stays within the company network. Print jobs

are only released to a selected printer once a user has authenticated at that device. The spool file is deleted automatically from a user's PC once it has been printed.

Mobile Printing

Users can print jobs from their mobile devices, smartphones or tablets. This can either be done by sending the file to be printed as an email to uniFLOW Online or by directly using mobile job submission on the uniFLOW Online tenant. In case the file needs to be converted from its native format into a language the printer understands, this will happen within the regional data center in which the uniFLOW Online service is hosted, i.e. customer data does not leave the data center. Once converted, the original file is deleted. The converted file is held within the regional data center until released/printed by the user.

Scanning

Users can scan from any connected Canon imageRUNNER ADVANCE to either themselves or cloud scan destinations. When scanning, the captured document travels via the cloud to the selected scan destination. However, no scan content or images are stored in uniFLOW Online. Only the processing, if applicable, is done in uniFLOW Online. Regular users and administrators have no access to content or index data of the scanned document.

Role Concept

Each uniFLOW Online instance allows to define user roles for known user which restricts access to certain information or configuration options if necessary. That way, it can be assured that critical information is only available to those users who have to create, edit or update private data.

Additional Services / API

uniFLOW Online allows to provide information to external services via API calls. However, the sharing of data outside uniFLOW Online is secured by additional mechanisms. First of all, valid API calls are only possible while a user is logged in to uniFLOW Online. Secondly, before data can be shared, a sharing request needs to be accepted by the administrator. Without allowance no data is shared outside uniFLOW Online.

Print Job Processing

As uniFLOW Online does not store any print jobs, accounting data and configuration information is all that leaves the company network and is sent outwards. The transmission of print job file names is disabled by default which removes yet another potential security risk. In case file names are required, administrators can enable the transmission option.

Schedule 3

List of current subprocessors

NT-ware may use the following Affiliates and third parties to provide certain parts of the Services on Customer's (and its Affiliates) behalf:

Subprocessor	Location/Mechanism	Function
NT-ware USA, Inc.	105 Maxess Road, Suite S129 Melville N.Y. 11747 USA	maintenance & support services
NT-ware Asia, Pte. Ltd.	438 Alexandra Road #04-01 Alexandra Point 119958 Singapore	maintenance & support services
NT-ware Japan Inc.	2-4-11, Higashi Shinagawa, Shinagawa Tokyo, Japan, 140-0002	maintenance & support services
Microsoft Ireland Operations, Ltd.	One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521	cloud service provider